申請日期：	88.11.-6	案號：	88119395
類別：	G06F 11/06 , 13/00		

（以上各欄由本局填註）

發明專利說明書 451125

一、發明名稱	中文	感染電腦病毒檔案之追蹤檢測方法
	英文	
二、發明人	姓名（中文）	1. 蔡俊男
	姓名（英文）	1.
	國籍	1. 中華民國
	住、居所	1. 新竹市振興路54號3樓
三、申請人	姓名（名稱）（中文）	1. 神達電腦股份有限公司
	姓名（名稱）（英文）	1.
	國籍	1. 中華民國
	住、居所（事務所）	1. 新竹市科學工業園區研發二路1號
	代表人姓名（中文）	1. 苗豐強
	代表人姓名（英文）	1.

五、發明說明（1）

1. 創作領域：

本發明是關於一種電腦病毒之檢測方法，特別是指一種檢測電腦系統之基本輸出入系統之INT13h中斷向量位址是否被改變而判斷檔案是否感染電腦病毒之方法。當本發明檢測到任何企圖改變電腦系統之基本輸出入系統BIOS之INT13h中斷向量位址時，即可發出即時之病毒警告，以適時警告使用者該電腦已感染到電腦病毒。

2. 背景說明：

查電腦病毒概可分為常駐型病毒與非常駐型病毒兩種，不同之電腦病毒都有其特有的病毒型態、傳播途徑，這些電腦病毒對一電腦系統而言，都會造成不同程度的破壞。

當執行到一被感染有常駐型病毒的程式時，該病毒程式會將它自己常駐在電腦系統之記憶體之中，等到下一個程式要執行的時候，常駐在記憶體中的電腦病毒便會伺機去感染目前所要執行的程式。有些類型的電腦病毒是藉由攔截電腦系統之中斷向量來達到感染之目的。例如，在目前已知的大部份電腦病毒會去修改基本輸出入系統BIOS所提供的INT03h、INT13h或INT21h中斷向量，其最主要之目的就是達到感染的目的。當電腦病毒程式攔截到該中斷向量（例如INT13h）時，該病毒程式會改變該中斷向量之向量位址，並以一新副程式取代該中斷向量之功能，並以該新的副程式作為病毒傳佈之途徑。

中斷向量INT13h之功能是控制硬碟及軟碟之資料存取

五、發明說明 (2)

功能。此一中斷藉由暫存器AH中不同之函數值，可得到不同之磁碟I/O功能。例如當AH值為03h時，其功能係為寫入資料至磁碟之磁區，部份電腦病毒程式即常利用這個功能函數來破壞磁碟的分割磁區(Partition Sector)或寫入資料至其它磁區。又例如當AH值為05h時，其功能係為格式化硬碟，如果電腦病毒是利用此項功能，則在病毒發作的時侯會格式化(Format)硬碟。因此，若無法有效偵測電腦系統之病毒的話，則對於電腦之使用及資料之安全性將會有極大的威脅。

本發明概述:

因此，本發明之主要目的即提供一種檢測電腦病毒之方法，本發明之方法可以在檢測到任何企圖改變INT13h之向量位址之動作時，即可發出即時之病毒警告，以適時警告使用者該電腦可能已感染到電腦病毒。本發明之方法亦可用於日後未知病毒之追蹤檢測。

本發明之另一目的是提供一種檢測感染有電腦病毒之檔案之方法，其結合了中央處理器中相關之控制暫存器、斷點暫存器、除錯控制暫存器、除錯狀態暫存器等來執行病毒之檢測。

為達到本發明之上述目的，本發明所提供之感染有電腦病毒檔案之追蹤檢測方法，係首先在該電腦系統之記憶體中指定一記憶區，然後設定該中央處理器中各相關暫存器、判斷該中央處理器是否有除錯狀況產生、判斷中央處理器之除錯狀態暫存器中之對應中斷點條件是否被設定。

五、發明說明（3）

當中斷點條件已被設定時，即由堆疊中取得觸發該除錯狀況之指令位址，然後將該指令節區及偏移位址予以正規化、以及建立一記憶體控制區塊串列，並對前述之記憶體控制區塊之串列進行掃描以找出任何涵蓋到前述正規化之指令節區及偏移位址之程式。將該改變INT13h中斷向量之程式名稱及位址予以記錄。最後對該記憶區中之檔案內容進行掃描，若比對出與已知病毒碼相同之檔案內容，即警示使用者，若未比對出與已知病毒碼相同之檔案內容時，則可輸出該檔案內容，以作為日後未知病毒之追蹤檢測。

本發明之其它目的及其進一步之病毒檢測方法，將藉由以下之較佳實施例說明及附呈圖式，作進一步之說明，其中：

（一）圖式簡要說明：

圖一係顯示一包括有中央處理器、輸出入界面、磁碟裝置、記憶體之典型個人電腦簡化系統圖；

圖二係顯示中央處理器中各主要暫存器之示意圖；

圖三係顯示一Pentium級中央處理器內部相關暫存器之示意圖；

圖四係顯示本發明病毒檢測方法之流程圖；

圖五係接續圖四之流程圖。

（二）圖號說明：

1　中央處理器

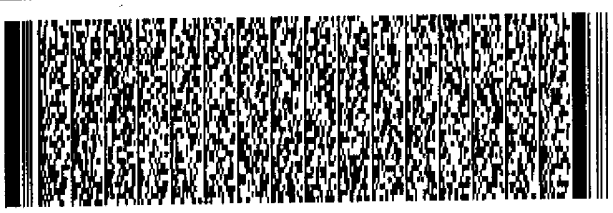
10　通用暫存器

五、發明說明（4）

11	狀態及指令暫存器
12	節區暫存器
13	控制暫存器組
14	除錯暫存器組
2	系統匯流排
21	位址匯流排
22	資料匯流排
23	控制匯流排
3	輸出入界面
4	磁碟裝置
5	記憶體
CR0~CR4	控制暫存器
DR0~DR3	除錯位址暫存器
DR6	除錯狀態暫存器
DR7	除錯控制暫存器

較佳實施例說明：

圖一係顯示一典型個人電腦系統中，包括有一中央處理器1、一輸出入界面3、一磁碟裝置4、一記憶體5間之簡化系統示意圖。該中央處理器1經由系統區域匯流排2及輸出入界面3而與磁碟裝置4連接，而中央處理器1則經由該系統匯流排2而與一記憶體5相連接。其中該系統匯流排2係包括有位址匯流排21、資料匯流排22、及控制匯流排23，以作為中央處理器2與各元件間之資料、位址信號、及控制信號之傳送路徑。



五、發明說明 (5)

在以下之實施例中，是以Intel公司Pentium級中央處理器作一較佳實施例說明，且該磁碟裝置4係可經由一IDE界面而與中央處理器1相連接。

參閱圖二所示，其係顯示一典型之中央處理器中各主要暫存器之示意圖。中央處理器內部之一般用途暫存器依其功能之不同，約略可分為通用暫存器10(General Purpose Register)、狀態及指令暫存器11(Status and Instruction Register)、節區暫存器12(Segment Register)。其中該通用暫存器10包括有數個十六位元暫存器AX、BX、CX、DX、BP、SP、SI、DI、以及數個八位元之暫存器AH、AL、BH、BL、CH、CL、DH、DL。這些暫存器一般是用來處理位元組資料。而較先進之中央處理器在處理32位元的資料時，可以使用八個32位元的通用暫存器EAX、EBX、ECX、EDX、EBP、ESP、ESI、EDI。

狀態及指令暫存器11包括有IP、FLAGS、EIP、EFLAGS暫存器，是用來指定欲執行指令、以及指示在執行指令後的結果狀態。

節區暫存器12包括有程式節區暫存器CS、堆疊節區暫存器SS、資料節區暫存器DS、額外資料節區暫存器ES、旗標節區暫存器FS、通用節區暫存器GS。這些暫存器可用來決定記憶體位址節區的基底位址。

在Pentium級中央處理器內部尚包括有其它系統暫存器，這些系統暫存器中，與本發明之病毒檢測方法有關之暫存器示於圖三中，其包括有控制暫存器組13及除錯暫存

五、發明說明 (6)

器組14。其中之控制暫存器組13中包括有數個控制暫存器CR0~CR4，其中控制暫存器CR4之位元定義中，共有位元0至位元6，其中之位元3乃為除錯擴展功能(Debugging Extension)之設定位元，當該位元設定為1時，乃啟動輸出入界面斷點除錯擴展功能，當該位元設定為0時，乃解除輸出入界面斷點除錯擴展功能。

除錯暫存器組14中包括有八個暫存器DR0~DR7，其中之DR0~DR3是作為除錯位址暫存器(Debug Address Resister)，每一個除錯位址暫存器中含32位元的斷點線性位址(Breakpoint Linear Address)。DR6是作為除錯狀態暫存器(Debug Status Register)，其可在除錯狀況產生時，告知該除錯狀況之條件。DR7係作為一除錯控制暫存器(Debug Control Register)，其可用來致能或禁能斷點功能、以及可用來設定斷點條件。

每一個除錯位址暫存器DR0~DR3皆有一些各自的控制位元(在除錯控制暫存器DR7中)，例如在DR7中之LEN位元值決定了斷點位址的存取長度，當LEN=00時，其存取長度為一個位元組，當LEN=01時其存取長度為二個位元組，當LEN=11時，其存取長度為四個位元組。又，DR7中之R/W之位元值決定在斷點位址上發生斷點的原因，當R/W=00時係表示指令碼存取，R/W=01時係表示資料寫入，當R/W=10時係表示I/O讀取或寫入，當R/W=11時是表示資料讀取與寫入。

以下將同時參閱圖一所示之系統架構圖、圖二及圖三

五、發明說明 (7)

所示之中央處理器內部暫存器組架構及圖四、圖五所示之控制流程圖，對本發明之病毒檢測方法作一詳細說明如后。

在程式啟始後，本發明首先於步驟100中，在該電腦系統之記憶體中指定一記憶區，此一記憶區可在後續之病毒檢測程序中用來保存該改變中斷向量INT13h之程式之名稱及其啟始位址。

接著在步驟101中進行中央處理器中各相關暫存器之設定，此步驟中包括：

1. 在中央處理器之任一個偵錯位址暫存器(DR0-DR3)中設定十六進位數值資料4Ch，該數值資料4Ch係用以指出INT13h中斷向量於中斷向量表中之記憶體位址所在(由於每個中斷向量佔4位元組大小，此值即由13h x 4而求得)。
2. 在中央處理器之除錯控制暫存器DR7之R/W位元(讀取/寫入控制位元)中設定數值01，其意謂啟動中央處理器在執行資料寫入時之中斷功能。
3. 在該除錯控制暫存器DR7之LEN位元(長度位元)中設定數值11，其數值係代表斷點位址之存取長度值是四個位元組。

在完成上述之相關暫存器資料設定之後，即執行步驟102，此一步驟是判斷是否有除錯狀況(Debug Exception)產生，若無，則繼續迴圈測試，若有，中央處理器會啟始一中斷向量INT01h之中斷服務程式，並執行下一步驟

五、發明說明 (8)

103，進一步判斷中央處理器中除錯狀態暫存器DR6之狀態，該除錯狀態暫存器DR6可反映斷點暫存器DR0-DR3的狀態。

在步驟103中，判斷中央處理器之除錯狀態暫存器DR6中之對應中斷點條件(Breakpoint Condition)是否被設定。若結果為否，則回到步驟102，若結果為是，則進行下一步驟104。

在步驟104中，由記憶體堆疊節區(Stack Segment)中取得觸發該除錯狀況之指令之節區及偏移位址(Segment & Offset)值。然後，在步驟105中，將該指令之節區及偏移位址予以正規化。

接著在步驟106中，建立一DOS之記憶體控制區塊(Memory Control Block， 簡稱MCB)串列。建立該記憶體控制區塊串列之方式，首先需呼叫DOS作業系統中之INT21h/AH=52h功能函數，在執行該INT21h/AH=52h功能函數之後，可於記憶體位址ES:〔BX-2〕取得第一個記憶體控制區塊之節區位址(16位元)，而由記憶體控制區塊所包含之區塊擁有者之PSP(程式前置區)節區位址及區塊長度等資訊，可進一步取得當時在記憶體中所有程式(Process)之位址與名稱。

在本發明之實施例中，該記憶體控制區塊之格式可為:

偏移位址 (Offset)	大小 (Size)	說明 (Description)

五、發明說明 (9)

00h	1 Byte	控制區塊之型式(若該區塊為最後一個，則其數值為5Ah，否則其數值為4Dh)。
01h	1 Word	控制區塊擁有者之PSP(程式前置區)節區位址。
03h	1 Word	區塊(Memory Block)之長度。
05h	3 bytes	未使用。
08h	8 bytes	區塊擁有者之程式名稱(Process Name)。

在圖五所示之步驟107中，對前述之記憶體控制區塊之串列(MCB List)進行掃描，以找出所在區域涵蓋前述正規化後節區及偏移位址之程式。

然後在步驟108中，將該改變INT13h中斷向量之程式名稱及位址予以記錄在步驟100中所指定之記憶區中。再於步驟109中，對該記憶區中之檔案內容進行掃描，並與已知病毒碼進行比對。

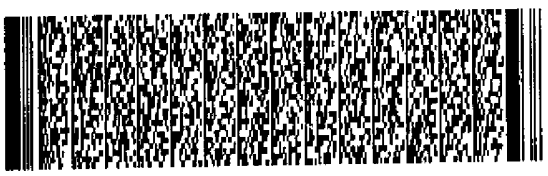
比對之結果，若並未檢測到相同於已知病毒碼的話(步驟110)，則執行步驟111，將該檔案之內容予以輸出，以作為日後未知病毒之追蹤檢測。若步驟110中之判別結果為是，則即時顯示該電腦病毒之名稱，以警示該電腦已感染電腦病毒。

藉由以上之病毒檢測方法以及利用中央處理器中相關之暫存器，使本發明可以有效即時檢測到任何企圖寫入至電腦系統的磁碟裝置之電腦病毒。一旦檢測到已知之電腦

五、發明說明（10）

病毒碼後，即可發出一警告，以適時警告使用者，若未比對到相符之已知電腦病毒時，則可以作為日後未知病毒之追蹤檢測。

因此，本發明所提供之電腦病毒檢測方法，確具高度之產業利用價值，可達到預期之功效，且在專利申請前亦未有相同或類似之技術公開在先，業已符合於發明專利之要件，爰依法提出發明專利之申請。



四、中文發明摘要　（發明之名稱：感染電腦病毒檔案之追蹤檢測方法）

一種感染電腦病毒檔案之追蹤檢測方法，係在該電腦系統之記憶體中指定一記憶區，然後設定該中央處理器中各相關暫存器、判斷該中央處理器是否有除錯狀況產生、判斷中央處理器之除錯狀態暫存器中之對應中斷點條件是否被設定。當中斷點條件已被設定時，即由堆疊中取得觸發該除錯狀況之指令位址，然後將該指令之節區及偏移位址予以正規化、及建立一記憶體控制區塊串列，並對前述記憶體控制區塊之串列進行掃描，以找出涵蓋到前述正規化之指令節區及偏移位址之程式。然後將該改變INT13h中斷向量之程式名稱及位址予以記錄。最後對該記憶區中之檔案內容進行掃描，並與已知病毒碼比對，若比對出與已知病毒碼相同之檔案內容，即警示使用者。

英文發明摘要　（發明之名稱：）

六、申請專利範圍

1. 一種感染電腦病毒檔案之追蹤檢測方法，係檢測企圖改變電腦系統之基本輸出入系統之INT13h中斷向量位址之電腦病毒程式，該電腦系統之中央處理器內部配置有控制暫存器、斷點暫存器、除錯控制暫存器、除錯狀態暫存器，該檢測方法包括下列步驟：

a. 在該電腦系統之記憶體中指定一記憶區；

b. 設定該中央處理器中各相關暫存器；

c. 判斷該中央處理器是否有除錯狀況產生，若無，則繼續迴圈測試，若有，則進一步判斷中央處理器之除錯狀態暫存器中之對應中斷點條件是否被設定；

d. 若該中央處理器之除錯狀態暫存器中之對應中斷點條件已被設定，則由記憶體堆疊節區中取得觸發該除錯狀況之指令之區及偏移位置；

e. 將該指令之節區及偏移位址予以正規化；

f. 建立一記憶體控制區塊串列；

g. 對該記憶體控制區塊之串列進行掃描，以找出涵蓋到前述正規化之指令節區及偏移位址之程式；

h. 將該改變INT13h中斷向量之程式名稱及位址予以記錄在步驟a中所指定之記憶區中；

i. 對該記憶區中之檔案內容進行掃描，並與已知病毒碼比對，若比對出與已知病毒碼相同之檔案內容，即警示使用者。

2. 如申請專利範圍第1項所述之感染電腦病毒檔案之追蹤

六、申請專利範圍

檢測方法，其中步驟b在設定該中央處理器中各相關暫存器之步驟包括：

b1. 在中央處理器之任一個偵錯位址暫存器中設定一預定數值；

b2. 在中央處理器之除錯控制暫存器之讀取/寫入控制位元中設定一預定數值；

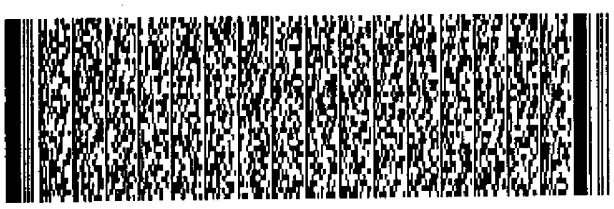
b3. 在該除錯控制暫存器之長度設定位元中設定一預定數值。

3. 如申請專利範圍第2項所述之感染電腦病毒檔案之追蹤檢測方法，其中步驟b1在任一個偵錯位址暫存器中所設定之預定數值為十六進位數值資料4Ch。

4. 如申請專利範圍第2項所述之感染電腦病毒檔案之追蹤檢測方法，其中步驟b2中，該中央處理器之除錯控制暫存器之讀取/寫入控制位元中所設定之預定數值為01，其意謂啟動中央處理器在執行資料寫入時之中斷功能。

5. 如申請專利範圍第2項所述之感染電腦病毒檔案之追蹤檢測方法，其中步驟b3中，該中央處理器之除錯控制暫存器之長度設定位元中所設定之預定數值為11，其係代表斷點位址之存取長度值是四個位元組。

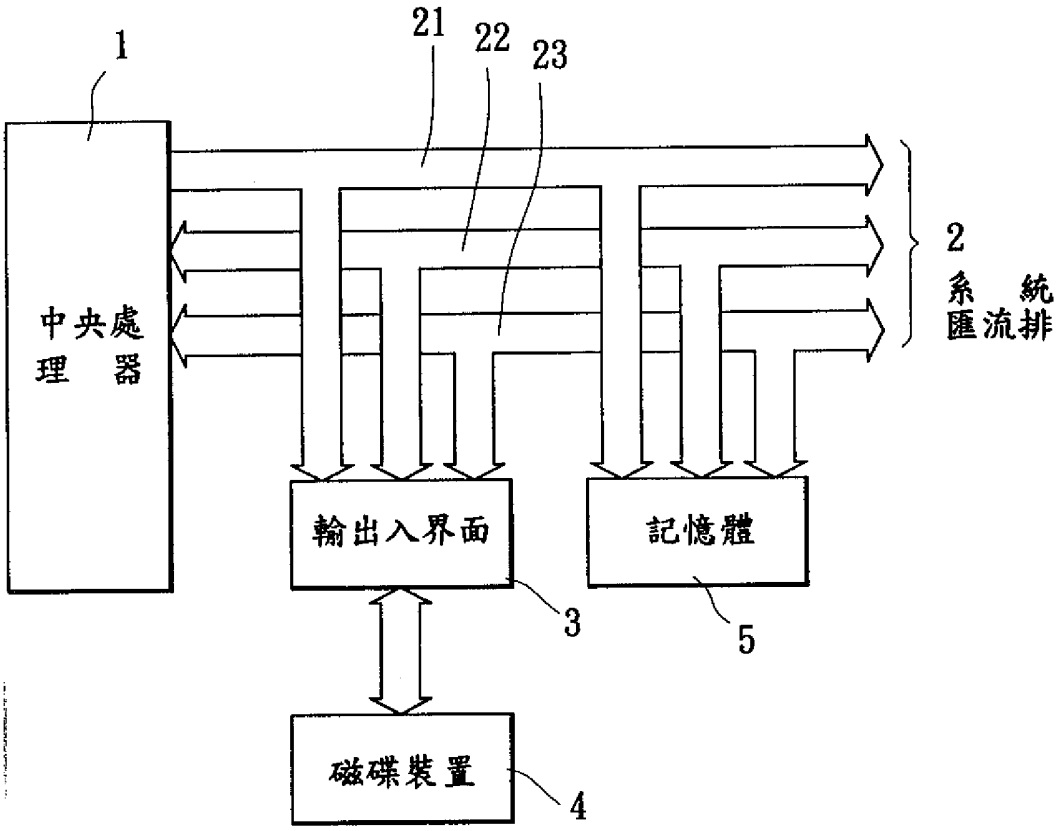
6. 如申請專利範圍第1項所述之感染電腦病毒檔案之追蹤



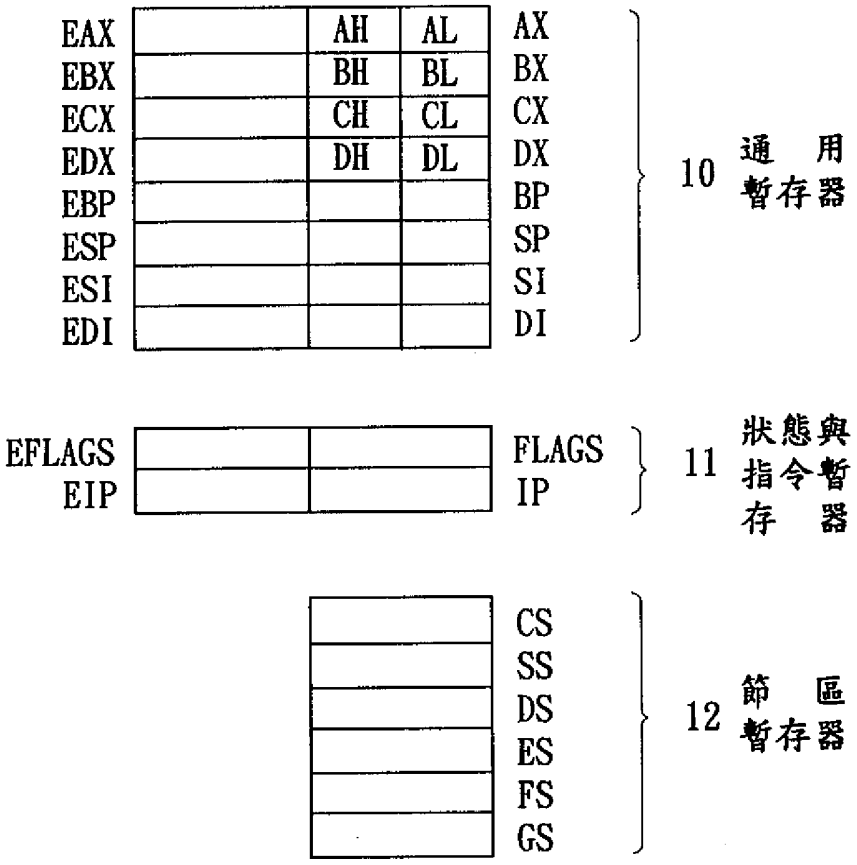
六、申請專利範圍

檢測方法，其中步驟f建立記憶體控制區塊串列係呼叫DOS作業系統中之INT21h/AH=52h功能函數。

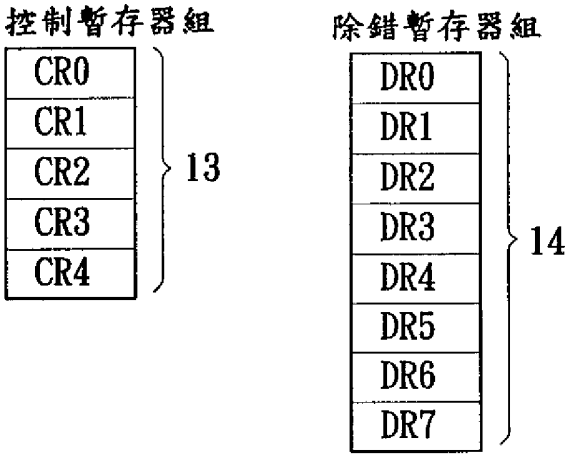
7. 如申請專利範圍第1項所述之感染電腦病毒檔案之追蹤檢測方法，其中步驟I中，若在對該記憶區中之檔案內容進行掃描及比對時，並未比對出與已知病毒碼相同之檔案內容時，其更包括輸出該檔案內容，以作為日後未知病毒之追蹤檢測。



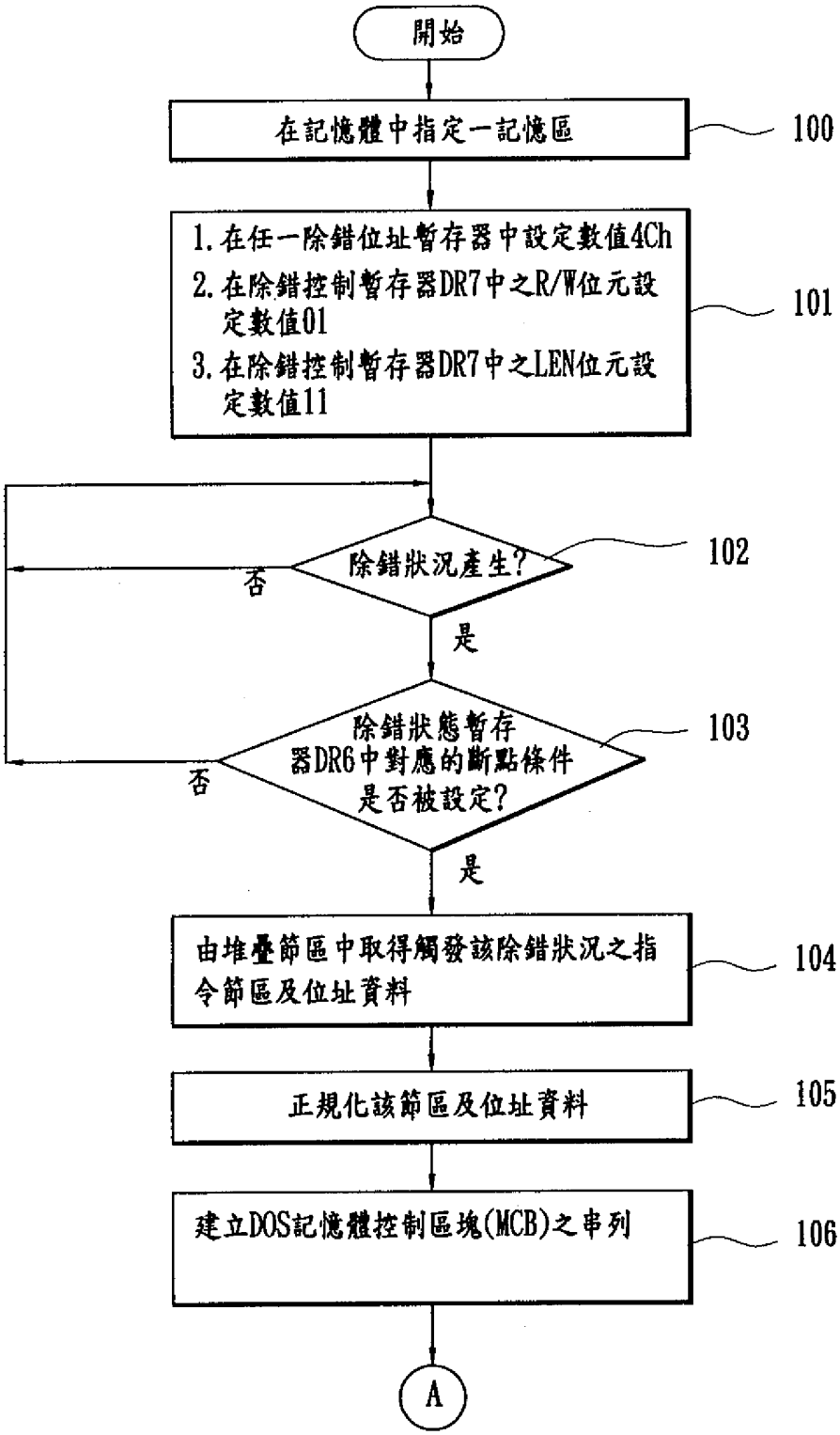
圖一


EAX
EBX
ECX
EDX
EBP
ESP
ESI
EDI
AH
AL
BH
BL
CH
CL
DH
DL
AX
BX
CX
DX
BP
SP
SI
DI
10
通用暫存器
EFLAGS
EIP
FLAGS
IP
11
狀態與指令暫存器
CS
SS
DS
ES
FS
GS
12
節區暫存器

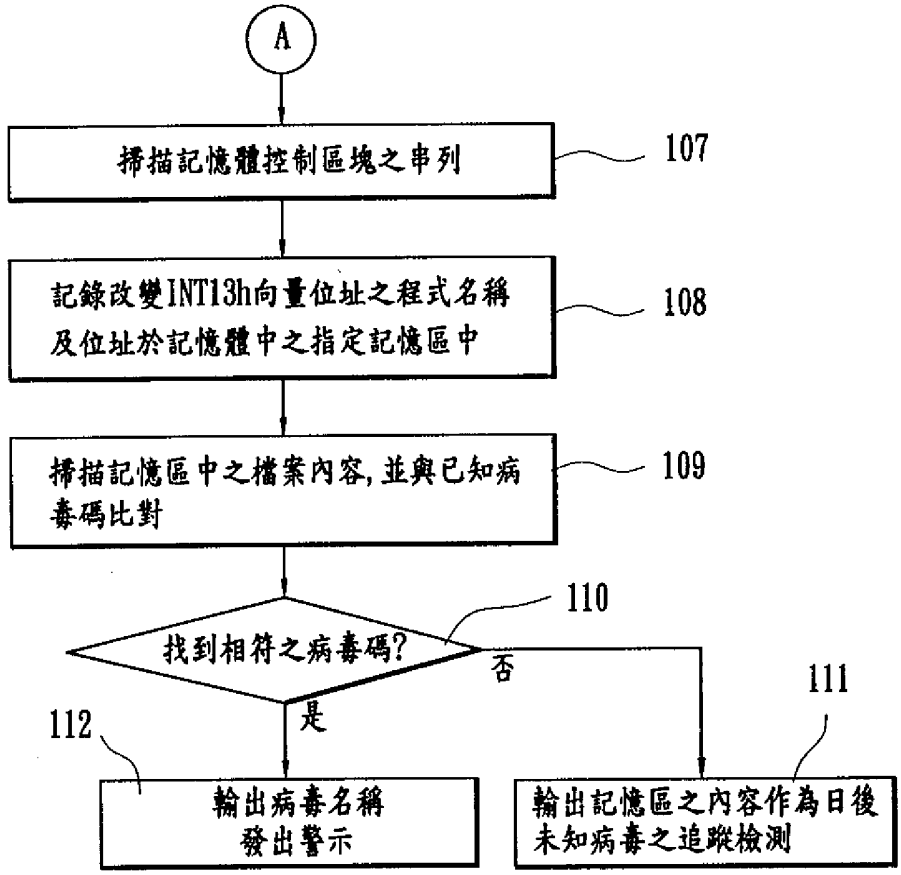
圖二


控制暫存器組
CR0
CR1
CR2
CR3
CR4
13
除錯暫存器組
DR0
DR1
DR2
DR3
DR4
DR5
DR6
DR7
14

圖三


開始
在記憶體中指定一記憶區
100
1. 在任一除錯位址暫存器中設定數值4Ch
2. 在除錯控制暫存器DR7中之R/W位元設定數值01
3. 在除錯控制暫存器DR7中之LEN位元設定數值11
101
除錯狀況產生?
102
否
是
除錯狀態暫存器DR6中對應的斷點條件是否被設定?
103
否
是
由堆疊節區中取得觸發該除錯狀況之指令節區及位址資料
104
正規化該節區及位址資料
105
建立DOS記憶體控制區塊(MCB)之串列
106
A

圖四


A
掃描記憶體控制區塊之串列
107
記錄改變INT13h向量位址之程式名稱
及位址於記憶體中之指定記憶區中
108
掃描記憶區中之檔案內容,並與已知病
毒碼比對
109
找到相符之病毒碼?
110
否
是
111
112
輸出病毒名稱
發出警示
輸出記憶區之內容作為日後
未知病毒之追蹤檢測

圖五